Project Title: Security with AWS: Identity and Access Management

Instructor: Olayinka Arimoro

Task 3: Create IAM users from the CLI

- **Confirm or verify AWS installation using:**
  ```
  aws --version
  ```

- **Configure AWS account using:**
  ```
  aws configure
  ```

- **Create a user called Matt:**
  ```
  aws iam create-user --user-name Matt
  ```

- **Create a user called Sarah:**
  ```
  aws iam create-user --user-name Sarah
  ```

- **Create a user called Deborah:**
  ```
  aws iam create-user --user-name Deborah
  ```

Task 4: Create IAM groups and add users to the groups

- **Create the cloud security team group:**
  ```
  aws iam create-group --group-name CloudSecurityTeam
  ```

- **Add user Matt to this group:**
  ```
  aws iam add-user-to-group --group-name CloudSecurityTeam --user-name Matt
  ```

- **Add user Sarah to this group:**
  ```
  aws iam add-user-to-group --group-name CloudSecurityTeam --user-name Sarah
  ```

- **Attach the AmazonS3FullAccess policy to this group:**
  ```
  aws iam attach-group-policy --group-name CloudSecurityTeam --policy-arn "arn:aws:iam::aws:policy/AmazonS3FullAccess"
  ```

Task 7: Create an IAM role for an AWS service

- **List S3 buckets:**
  `aws s3 ls`

- **Get EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/`

- **Get the public host name from the EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/public-hostname`

- **Get the instance type from the EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/instance-type`

- **Get the IAM information from the EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/iam/info`

- **Get the attached IAM role name from the EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/iam/security-credentials/`

- **Get the STS security credentials for an IAM role from the EC2 instance metadata:**
  `curl http://169.254.169.254/latest/meta-data/iam/security-credentials/[PUT_THE_ROLENAME]`

Task 8: Use IAM roles to grant AWS cross-account access

- **Link to AWS Management Console:**
  https://auditteamcompanyxyz.signin.aws.amazon.com/console

- **Username:** AuditTeamAdmin

- **Password:** @AWSSampleIAMUser23

Task 9: Use IAM roles to grant AWS cross-account access with external ID

- **Configure the AWS account AuditTeamAdmin:**
  ```
  aws configure
  ```

  Access key ID: AKIA3GJ7MXIW7JTNHKN6
  Secret Access Key: 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

- **Get the caller identity:**
  ```
  aws sts get-caller-identity
  ```

- **List S3 buckets:**
  ```
  aws s3 ls
  ```

- **Get temporary security credentials:**
  ```
  aws sts assume-role --role-arn
  arn:aws:iam::[PUT_THE_ACCOUNTID]:role/[PUT_THE_ROLENAME] --role-
  session-name [PUT_A_SESSIONNAME] --external-id [PUT_EXTERNALID]
  ```

- **Set the access key ID:**
  ```
  set AWS_ACCESS_KEY_ID=[PUT_ACCESSKEYID]
  ```

- **Set the secret access key:**
  ```
  set AWS_SECRET_ACCESS_KEY=[PUT_SECRETACCESSKEY]
  ```

- **Set the session token:**
  ```
  set AWS_SESSION_TOKEN=[PUT_SESSIONTOKEN]
  ```

- **List buckets and objects:**
  ```
  aws s3 ls
  aws s3 ls s3://[PUT_BUCKETNAME]
  ```

- **Delete an S3 bucket:**
  ```
  aws s3 rb s3://[PUT_BUCKETNAME]
  ```

- **To delete objects in a bucket or your local directory:**
  ```
  aws s3 rm s3://bucket-
  name/[PUT_BUCKETNAME]/[PUT_FILENAME.EXTENSION]
  ```

Task 10: Revoke an IAM role

- **List S3 buckets:**

```
aws s3 ls
```

Task 11: Setting permissions boundary

- **Policy to prevent James from changing his own permissions:**

```
{
	"Version": "2012-10-17",
	"Statement": [
		{
			"Sid": "CreateOrChangeOnlyWithBoundary",
			"Effect": "Allow",
			"Action": [
				"iam:PutUserPermissionsBoundary",
				"iam:PutUserPolicy",
				"iam:DeleteUserPolicy",
				"iam:AttachUserPolicy",
				"iam:DetachUserPolicy",
				"iam:CreateUser"
			],
			"Resource": "*",
			"Condition": {
				"StringEquals": {
					"iam:PermissionsBoundary":
"arn:aws:iam::[PUT_ACCOUNTID]:policy/userboundary"}}
		},
		{
			"Sid": "CloudWatchAndOtherIAMTasks",
			"Effect": "Allow",
			"Action": [
			    "cloudwatch:*",
				"iam:GetUser",
				"iam:ListUsers",
				"iam:DeleteUser",
				"iam:UpdateUser",
				"iam:CreateAccessKey",
				"iam:CreateLoginProfile",
				"iam:GetAccountPasswordPolicy",
				"iam:GetLoginProfile",
				"iam:ListGroups",
				"iam:ListGroupsForUser",
				"iam:CreateGroup",
				"iam:GetGroup",
				"iam:DeleteGroup",
				"iam:UpdateGroup",
				"iam:CreatePolicy",
				"iam:DeletePolicy",
```

```
                    "iam:DeletePolicyVersion",
                    "iam:GetPolicy",
                    "iam:GetPolicyVersion",
                    "iam:GetUserPolicy",
                    "iam:GetRolePolicy",
                    "iam:ListPolicies",
                    "iam:ListPolicyVersions",
                    "iam:ListEntitiesForPolicy",
                    "iam:ListUserPolicies",
                    "iam:ListAttachedUserPolicies",
                    "iam:ListRolePolicies",
                    "iam:ListAttachedRolePolicies",
                    "iam:SetDefaultPolicyVersion",
                    "iam:SimulatePrincipalPolicy",
                    "iam:SimulateCustomPolicy"
                ],
    "NotResource":"arn:aws:iam::[PUT_ACCOUNTID]:user/[PUT_USERNAME]"
        },
        {
            "Sid": "NoboundaryPolicyEdit",
             "Effect": "Deny",
             "Action": [
                    "iam:CreatePolicyVersion",
                    "iam:DeletePolicy",
                    "iam:DeletePolicyVersion",
                    "iam:SetDefaultPolicyVersion"
             ],
             "Resource": [
              "arn:aws:iam::[PUT_ACCOUNTID]:policy/userboundary",
              "arn:aws:iam::[PUT_ACCOUNTID]:policy/adminboundary"
              ]
        },
        {
            "Sid": "NoboundaryUserDelete",
             "Effect": "Deny",
             "Action": "iam:DeleteUserPermissionsBoundary",
             "Resource": "*"
        }
    ]
}
```

Task 12: Revoke an IAM role

- **Create policy to deny CreateBucket:**

```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Sid": "VisualEditor0",
                  "Effect": "Deny",
                  "Action": "s3:CreateBucket",
                  "Resource": "*"
            }
      ]
}
```

- **Link to IAM Policy Simulator:**
  https://policysim.aws.amazon.com/